Number Theory: Diophantine Geometry

Number Theory, the study of the integers, is the oldest branch of pure mathematics, and also the largest. There are many questions to ask, about individual numbers and their properties, about operations on numbers, about relations between numbers, about sets of numbers, about patterns in sequences of numbers, and so on. Number Theory is famous for generating easy-to-ask, hard-to-answer questions, and that is one reason for its popularity.

Multiplication is the most interesting operation on integers. Number Theory treats factoring and divisibility, and prime numbers. The ancient Greeks knew how many primes there are, and discovered how they are distributed among the integers as a whole.

Number theory (or arithmetic or higher arithmetic) is a branch of pure mathematics devoted primarily to the study of the integers and arithmetic that will give a domain of a function positive integers and will give the range of this same function a complex number. German mathematician Carl Friedrich Gauss (1777–1855) said, 'Mathematics is the queen of the sciences—and number theory is the queen of mathematics.' Number theorists study prime numbers as well as the properties of objects made out of integers (for example, rational numbers) or defined as generalizations of the integers (for example, algebraic integers). Number theory aims to understand the properties of integer systems in spite of their apparent complexity.

Integers can be considered either in themselves or as solutions to equations. Questions in number theory are often best understood through the study of analytical objects that encode properties of the integers, primes or other number-theoretic objects in some fashion (analytic number theory). One may also study real numbers in relation to rational numbers.

The older term for number theory is arithmetic. By the early twentieth century, it had been replaced by 'number theory'. The use of the term arithmetic for number theory regained some ground in the second half of the 20th century, arguably in part due to French influence. In particular, arithmetical is preferred as an adjective to number-theoretic.

Origin:

1-Diophantus:

Very little is known about Diophantus of Alexandria (the author of a series of books called Arithmetica, many of which are now lost. His texts deal with solving algebraic equations); he probably lived in the third century CE. Six out of the thirteen books of Diophantus's Arithmetica survive in the original Greek; four more books survive in an Arabic translation. The Arithmetica is a collection of worked-out problems where the task is invariably to find rational solutions to a system of polynomial equations (x , y) = z 2 {displaystyle f(x,y)=z^{2}} f (x , y , z) = w 2 {displaystyle f(x,y,z)=w^{2}}. Thus, nowadays, we speak of Diophantine equations when we speak of polynomial equations to which rational or integer solutions must be found.

One may say that Diophantus was studying rational points, that is, points whose coordinates

are rational—on curves; however, unlike the Greeks of the Classical period, who did what we would now call basic algebra in geometrical terms, Diophantus did what we would now call basic algebraic geometry in purely algebraic terms. In modern language, what Diophantus did was to find rational parameterization (the process of finding the equation of a curve) of varieties. f (x 1 , x 2 , x 3) = 0. {displaystyle f(x_{1},x_{2},x_{3})=0.}

Diophantus also studied the equations of some non-rational curves, for which no rational parameterization is possible. He managed to find some rational points on these curves (elliptic curves, as it happens, in what seems to be their first known occurrence) by means of what amounts to a tangent construction: translated into coordinate geometry (which did not exist in Diophantus's time), his method would be visualized as drawing a tangent to a curve at a known rational point, and then finding the other point of intersection of the tangent with the curve; that other point is a new rational point.

While Diophantus was concerned largely with rational solutions, he assumed some results on integer numbers, in particular, that every integer is the sum of four squares (though he never stated as much explicitly).

2-Arithmetic in the Islamic golden age:

In the early ninth century, the caliph Al-Ma'mun ordered translations of many Greek mathematical works. Diophantus's main works, the Arithmetica, was translated into Arabic by Qusta ibn Luqa (820–912). Part of the work al-Fakhri (by al-Karaj?, 953 – ca. 1029) builds on it to some extent.

Western Europe in the middle ages:

Other than a paper on squares in arithmetic progression by Fibonacci—who traveled and studied in north Africa and Constantinople—no number theory to speak of was done in western Europe during the Middle Ages. Matters started to change in Europe in the late Renaissance, thanks to a renewed study of the works of Greek antiquity. A catalyst was the textual correction and translation into Latin of Diophantus' Arithmetica.

Main subdivisions: (subdivision occurred in the early modern era)

1-Elementary tools:

The term elementary generally denotes a method that does not use complex analysis. For example, the prime number theorem was first proven using complex analysis in 1896, but an elementary proof was found only in 1949 by Erd?s and Selberg. Here as elsewhere, an elementary proof may be longer and more difficult for most readers than a non-elementary one.

Number theory has the reputation of being a field many of whose results can be stated to the normal individual. At the same time, the proofs of these results are not particularly accessible, in part because the range of tools they use is, if anything, unusually broad within mathematics.

2-Analytic number theory:

Analytic number theory may be defined:

- in terms of its tools, as the study of the integers by means of tools from real and complex analysis; or
- in terms of its concerns, as the study within number theory of estimates on size and density, as opposed to identities.

The following are examples of problems in analytic number theory: the prime number theorem, the Goldbach conjecture (or the twin prime conjecture, or the Hardy–Littlewood conjectures), the Waring problem and the Riemann hypothesis. Some of the most important tools of analytic number theory are the circle method, sieve methods and L-functions (or, rather, the study of their properties). The theory of modular forms also occupies an increasingly central place in the toolbox of analytic number theory.

One may ask analytic questions about algebraic numbers, and use analytic means to answer such questions; it is thus that algebraic and analytic number theory intersect. For example, one may define prime ideals (generalizations of prime numbers in the field of algebraic numbers) and ask how many prime ideals there are up to a certain size. This is an example of a general procedure in analytic number theory: deriving information about the distribution of a sequence (here, prime ideals or prime numbers) from the analytic behavior of an appropriately constructed complex-valued function.

3-Algebraic number theory:

An algebraic number is any complex number that is a solution to some polynomial equation f (x) = 0 {displaystyle f(x)=0} with rational coefficientsx {displaystyle x} x 5 + (11 / 2) x 3 ? 7 x 2 + 9 = 0 {displaystyle x^{5}+(11/2)x^{3}-7x^{2}+9=0}. Fields of algebraic numbers are also called algebraic number fields, or shortly number fields. Algebraic number theory studies algebraic number fields. Thus, analytic and algebraic number theory can and do overlap: the former is defined by its methods, the latter by its objects of study.

It could be argued that the simplest kind of number fields (specifically quadratic fields, a quadratic field consists of all numbers of the form a + b d {displaystyle a+b{sqrt {d}}} a {displaystyle a} b {displaystyle b} are rational numbers and d {displaystyle d} is a fixed rational number whose square root is not rational.) For that matter, the 11th-century chakravala method amounts—in modern terms—to an algorithm for finding the units of a real quadratic number field.

The grounds of the subject as we know it were set in the late nineteenth century, when ideal numbers, the theory of ideals and valuation theory were developed; these are three complementary ways of dealing with the lack of unique factorization in algebraic number fields.? 5 {displaystyle {sqrt {-5}}} 6 {displaystyle 6} 6 = 2 ? 3 {displaystyle 6=2cdot 3} 6 = (1 + ? 5) (1 ? ? 5) {displaystyle 6=(1+{sqrt {-5}})(1-{sqrt {-5}})} 2 {displaystyle 2} 3 {displaystyle 3} 1 + ? 5 {displaystyle 1+{sqrt {-5}}} 1 ? ? 5 {displaystyle 1-{sqrt {-5}}}

Number fields are often studied as extensions of smaller number fields: a field L is said to be an extension of a field K if L contains K. (For example, the complex numbers C are an extension of the reals R, and the reals R are an extension of the rationals Q.) Classifying the possible extensions of a given number field is a difficult and partially open problem. An example of an active area of research in algebraic number theory is Iwasawa theory.

4-Diophantine geometry:

The central problem of Diophantine geometry is to determine when a Diophantine equation (a polynomial equation in which there are 2 or more unknowns) has solutions, and if it does, how many. The approach taken is to think of the solutions of an equation as a geometric object.

For example, an equation in two variables defines a curve in the plane. More generally, an equation, or system of equations, in two or more variables defines a curve or a surface. In Diophantine geometry, one asks whether there are any rational points (points all of whose coordinates are rational numbers) or integral points (points all of whose coordinates are integers) on the curve or surface. If there are any such points, the next step is to ask how many there are and how they are distributed. A basic question in this direction is if there are finitely or infinitely many rational points on a given curve (or surface).x 2 + y 2 = 1 , {displaystyle x^{2}+y^{2}=1,} (x , y) {displaystyle (x,y)}a 2 + b 2 = c 2 {displaystyle a^{2}+b^{2}=c^{2}} x = a / c {displaystyle x=a/c} y = b / c {displaystyle y=b/c} x 2 + y 2 = 1 {displaystyle x^{2}+y^{2}=1} f (x , y) = 0 {displaystyle f(x,y)=0} f {displaystyle f} f (x , y) = 0 {displaystyle f(x,y)=0} f (x , y) = 0 {displaystyle f(x,y)=0} f (x , y) = 0 {displaystyle f(x,y)=0}

There is also the closely linked area of Diophantine approximations: given a number Xx {displaystyle x}, then finding how well can it be approximated by rational numbers. This question is of special interest if X x {displaystyle x} XXis an algebraic number. If x {displaystyle x} X cannot be well approximated, then some equations do not have integer or rational solutions. Moreover, several concepts (especially that of height) turn out to be critical both in Diophantine geometry and in the study of Diophantine approximations.

Other subfields:

Computational number theory:

While the word algorithm goes back only to certain readers of al-Khw?rizm?, careful descriptions of methods of solution are older than proofs: such methods (that is, algorithms) are as old as any recognizable mathematics—ancient Egyptian and Chinese—whereas proofs appeared only with the Greeks of the classical period. a x + b y = c {displaystyle ax+by=c} .

Calculating the number theory is difficut, but the difficulty of calculating it can be useful: modern protocols for encrypting messages depend on functions that are known to all, but whose inverses are known only to a chosen few, and would take one too long a time to figure out on one's own. For example, these functions can be such that their inverses can be calculated only if certain large integers are factorized. While many difficult computational problems outside number theory are known, most working encryption protocols nowadays are based on the difficulty of a few number-theoretical problems.

Applications:

The number-theorist Leonard Dickson (1874–1954) said 'Thank God that number theory is unsullied by any application'. Elementary number theory is taught in courses for computer scientists; on the other hand, number theory also has applications to the continuous in numerical analysis (studying algorithms that use numerical approximations). As well as the well-

known applications to cryptography, there are also applications to many other areas of mathematics.

Summary:

We can say that the number theory was based on the efforts and the hard work of Diophantus, so we can call him the father of the number theory. Many scientists consider Mathematics the queen of the sciences and the number theory the queen of mathematics. The number theory has origin in the Islamic golden age as well, but there was no evidence that it had an origin in Europe's middle age or at least not before the Resonance. There are many subdivisions of the number theory but these division only appeared after the early modern era. Mathematics is used in every science field and therefore it has many applications across many fields. We even learn it in School when we study the quadratic functions or factorizations. Computer science students also study the number theory in various courses.